UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,317	03/09/2004	Shawn A.P. Smith	T00107	2095

33438 7590 06/25/2008
HAMILTON & TERRILE, LLP
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER	
HWA, SHYUE JIUNN	
ART UNIT	PAPER NUMBER
2163	

NOTIFICATION DATE	DELIVERY MODE
06/25/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@hamiltonterrile.com
seaton@hamiltonterrile.com
tmunoz@hamiltonterrile.com

Office Action Summary	**Application No.** 10/796,317	**Applicant(s)** SMITH ET AL.	
	Examiner JAMES HWA	**Art Unit** 2163	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _03 March 2008_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-20_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-20_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending in this office action. This action is responsive to Applicant's application filed 03/03/2008.

Response to Arguments

2. Applicant's arguments filed 03/03/2008 have been full considered but are not persuasive.

Applicant argued that claim 8-10 clearly fits within either the "machine" or "manufacture" categories recited in 35 U.S.C. § 101. Thus, applicant submits that such claims are statutory.

Examiner respectfully disagrees because the "one recordable medium" in claims 8-10 are intend the “medium” to include signals (instant specification page 5, paragraph 0023) and disclosed “implemented in software stored on a computer-readable medium and executed as a computer program on a general purpose or special purpose computer, the processing of **session-based log files**” (instant specification page 8, paragraph 0028). Thus, U.S.C. 101 rejection is maintained in this Office Action.

Applicant argued that, Kaler does not teach the “retrieving a subset of log file entries from the memory” in claim 1. Examiner respectfully disagrees.

Kaler teaches filter reduction is the process of modifying or creating a new version of a Boolean expression by binding a subset of the variables within the expression (page 13, paragraph 0215). The user made a time selection in the performance view window over a period of time where CPU behavior was in question. The animated application model or process diagram highlights the entities/processes involved in the selection. The event log window highlights all events in the specified time range, part (e.g. subset) of which represent a call tree (page 20, paragraph 0306).

Applicant argued that, Kaler does not teach the “processing each entry in the memory to identify entries in the subset of log file entries that belong to a complete client session” in claim 1. Examiner respectfully disagrees.

Kaler teaches the set of APIs includes an interface that enables the operating system to read any one or more of several fields in the application. These fields include arguments, causality i.d., dynamic event data, exception, return value, source process, source process name, source session, target process, target process name and target session (page 15, paragraph 0246).

The function of an in-process event creator (IEC) is to monitor the executing process for particular situations that occur which the developer wants to be monitored and to create an event that can be captured and later analyzed. The function of a dynamic event creator (DEC) monitors some aspect of the system operation that the developer wants to be monitored on a periodic or time basis (e.g. subset) and creates an event that can also be captured and later analyzed (page 2, paragraph 0027).

Applicant argued that, Kaler does not teach the “processing each entry in the memory to identify entries in the subset of log file entries that belong to a complete client session” in claims 2 and 4. Examiner respectfully disagrees.

Kaler teaches it's basically a unique i.d. to identify a particular stream of calls and to sort them out. It says that this Call goes with this Return, and that this Enter goes with this Leave. The VSA knows from the Causality i.d. that these are all somehow interrelated (page 11, paragraph 0186).

For the above reason, examiner believed that rejection of the last Office Action was proper.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of the title.

3. Claims 8-10 are rejected under 35 U.S.C.101 because the language of the claim raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practice application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C 101.

As to claims 8-10, "an article of manufacture having at least one recordable medium", the medium includes signal and carrier wave (page 5, paragraph 0023). As such, the claims are drawn to a form of signal. Signal is not one of the four categories of invention and therefore this claim(s) is/are not statutory. Thus, U.S.C 101 rejection is maintained in this Office Action.

The claims fail to place the invention squarely within one statutory class of invention. On page 5, paragraph 0023 of the instant specification, applicant has provided evidence that applicant intends the "medium" to include signals. As such, the claims are drawn to a form of energy. Energy is not one of the four categories of invention and therefore this claim(s) is/are not statutory. Energy is not a series of steps or acts and thus is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefor not a composition of matter.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2 and 4 are rejected under 35 U.S.C. 102(e) as being anticipated by Kaler et al. (US Patent Application No. 2003/0061541 A1, hereinafter “Kaler).

As to claim 1, Kaler teaches the claimed limitations:

“A method for grouping log file entries by session” as a method and apparatus for analyzing the performance of a data processing system (page 1, paragraph 0002).

The Visual Studio Analyzer (VSA) includes an efficient mechanism for collecting and transmitting the data to a central log (page 22, paragraph 0339). Logs from multiple machines must be merged and sorted (page 1, paragraph 0015).

API for generating events from begin session to end session (page 16, paragraph 0250-0252).

“Storing a log file of entries in a memory, each of said entries identifying a client request to a server” as when the user's specified trigger condition is detected, the LEC can immediately transmit all of the buffered events to the VSA for logging (page 12, paragraph 0204). The client program sends a message to the server with appropriate arguments, and the server returns a message containing the results of the program executed (page 5, paragraph 0083).

“Retrieving a subset of log file entries from the memory” as statements in the code and having the application write to a log file what was going on at different places in the network. Then all of the log files would need to be collected, merged, and sorted (page 1, paragraph 0001). The VSA maintains a log of all of the events that have been collected (page 18, paragraph 0283).

Filter reduction is the process of modifying or creating a new version of a Boolean expression by binding a subset of the variables within the expression (page 13, paragraph 0215). The user made a time selection in the performance view window over a period of time where CPU behavior was in question. The animated application model or process diagram highlights the entities/processes involved in the selection. The event log window highlights all events in the specified time range, part (e.g. subset) of which represent a call tree. The timeline window highlights the specified time range as well as shows performance peaks, and the summary window tallies the events in the time range and presents a summary (page 20, paragraph 0306).

“Processing each entry in the memory to identify entries in the subset of log file entries that belong to a complete client session” as some important pre-defined event fields are the Machine, Process, Entity, Instance (Session in the APIs) (page 9, paragraph 0139). The set of APIs includes an interface that enables the operating system to read any one or more of several fields in the application. These fields include arguments, Causality i.d., dynamic event data, exception, return value, source process, source process name, source session, target process, target process name and target session (page 15, paragraph 0246).

The function of an in-process event creator (IEC) is to monitor the executing process for particular situations that occur which the developer wants to be monitored and to create an event that can be captured and later analyzed. The function of a DEC monitors some aspect of the system operation that the developer wants to be monitored on a periodic or time basis (e.g. subset) and creates an event that can also be captured and later analyzed (page 2, paragraph 0027).

“Grouping entries in the subset that belong to a complete client session” as behind this visual depiction of the application model, the VSA maintains a log of all of the events that have been collected (page 18, paragraph 0283). By selecting the Collect tab, the user can quickly select the desired information to analyze. More complex queries can be generated by creating groups of selections using the OR tabs (page 14, paragraph 0232).

There exist known tools called profilers. These look at a single executing software application and try to understand its performance. They do this either by monitoring the program or else they hook into the program they are monitoring and generate events each time a program subcomponent commences or completes (page 2, paragraph 0019).

A transition occurs when one entity turns execution over to another to complete a specific task. The transition comprises four events, a Call event, an Enter event, a Leave event, and a Return event (page 10, paragraph 0172). When process is applied for both the source and the target, it is possible to collect together four events into the standard group of CALL/ENTER/LEAVE/RETURN (page 11, paragraph 0188).

As to claim 2, Kaler teaches the claimed limitations:

“A complete client session is identified by identifying all entries in the subset that are associated with a particular client session and that include both a beginning entry and an end entry” as BeginSession is called by an entity before it fires events to register its entity and instance names (source and session). EndSession is called by an entity after it completes firing events (page 1, paragraph 0251-0252).

It's basically a unique i.d. to identify a particular stream of calls and to sort them out. It says that this Call goes with this Return, and that this Enter goes with this Leave. The VSA knows from the Causality i.d. that these are all somehow interrelated (page 11, paragraph 0186).

As to claim 4, Kaler teaches the claimed limitations:

“An end entry for a client session is identified as any entry associated with that client session that has no other entries for that client session that occur within a session expiration window” as a number of user-customized, synchronized display windows show the constituent parts of the application execution and the corresponding performance characteristics, in both Gantt chart and graphical modes, either in real-time or post-mortem. A timeline window displays a visual representation of the timing of all related events. A summary window displays a distillation of the system performance during a user-selected time slice (page 3, paragraph 0038).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 3, 5-8, 11 and 14-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaler et al. (US Patent Application No. 2003/0061541 A1) as applied to claim 1 above, and further in view of Moran (US Patent No. 6,826,697 B1, hereinafter “Moran”).

As to claim 3, Kaler does not explicitly teach the claimed limitation “an end entry is identified as any entry that corresponds to a logout request”.

Moran teaches system utilities that display login session times are aware of this situation and use a boot record as an implicit logout record for any sessions open at the time. These programs also have another implicit close for login sessions: if there is a login record on the same line being used for an open session, the program implicitly closes that open session as of the time of the new login. Since there cannot be two active logins on the same line, the assumption is made that the logout record was somehow lost, and the new login is the best guess for the end of the previous one on that line (column 21, lines 11-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler an end entry is identified as any entry that corresponds to a logout request because that would allow a system administrator to be alerted whenever an entry matching any of the patterns he has specified is written to a designated log file, thereby substantially reducing his need to manually check the log file as taught by Moran (column 10, lines 43-46).

As to claim 5, Kaler does not explicitly teach the claimed limitation “an end entry for a client session is identified as any entry having a first timestamp value, where the difference between first timestamp value and a second timestamp value associated with a subsequent entry in the subset of log files exceeds a timeout value”.

Moran teaches the analysis engine then checks the timestamps on files in each user's home directory for consistency with the recorded login sessions. The password table enumerates the users, their home directories, and their login shells. The last-access times on the RC files for the login shell are compared to the user's last recorded login (column 26, lines 26-32).

This access time is compared to the timestamps on files that the command is expected to access. If those timestamps are earlier than the last-access time on the SetUID command, this is evidence that a SetUID buffer overflow attack may have occurred (column 34, lines 52-56).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler an end entry for a client session is identified as any entry having a first timestamp value because that would allow the operator to examine the transaction history, but do not provide the context needed to effectively reevaluate the decisions as taught by Moran (column 32, lines 22-25).

As to claim 6, Although Kaler teaches a transition occurs when one entity turns execution over to another to complete a specific task (page 10, paragraph 0172). EndSession is called by an entity after it completes firing events (page 16, paragraph 0252).

Kaler does not explicitly teach the claimed limitation “outputting all entries in the subset of log file entries that do not belong to a complete client session as raw log data”.

Moran teaches real-time systems are able to assume that the data they are operating on is accurate and complete within the expectations of the systems (column 9, lines 6-8). The stereotypical pattern is that when a valid username-password pair is entered, the login process writes a record to the utmp and wtmp files and updates the lastlog file. The utmp file tracks that are currently logged in and the wtmp file provide a historical record, including both completed login sessions and active sessions (column 19, lines 60-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler outputting all entries in the subset of log file entries that do not belong to a complete client session because that would allow real-time monitoring of larger volumes of traffic as taught by Moran (column 2, lines 56-57).

As to claim 7, although Kaler teaches incomplete information is stored specially, and when other incomplete data arrives, there is an attempt to pair up the incomplete data using pre-defined heuristics (page 18, paragraph 0275).

Kaler does not explicitly teach the claimed limitation “outputting as raw log data all entries in the subset of log file entries that belong to an incomplete client session which has a beginning entry but no end entry”.

Moran teaches because of the complexity of the data, an embodiment may use a hybrid approach in its analysis engine. Incomplete data presents serious difficulties for a backward-chaining (column 38, lines 59-62).

The lastlog file contains the time of the last login for each user, and the previous value is written to the user's terminal as part of the hello message. When the user logs out, the getty process removes the corresponding entry from the utmp file and writes a session-end record to the wtmp file (column 19, line 66 to column 20, line 3). The file system occasionally gets corrupted, either from a hardware fault or because the system failed to complete a sequence of writes operations (column 30, lines 55-57).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler outputting as raw log data all entries in the subset of log file entries that belong to an incomplete client session because that would allow real-time monitoring of larger volumes of traffic as taught by Moran (column 2, lines 56-57).

As to claim 8, Kaler teaches the claimed limitations:

"An article of manufacture having at least one recordable medium having stored thereon executable instructions and data which, when executed by at least one processing device, cause the at least one processing device" as a method and apparatus for analyzing the performance of a data processing system (page 1, paragraph 0002).

Data is stored and retrieved for reading from and writing to hard-disk-drive interface, magnetic disk drive for reading from and writing to a removable magnetic disk, and optical disk drive for reading from and/or writing to a removable optical disk such as a CD-ROM, DVD or other optical medium (page 5, paragraph 0089).

"Read a plurality of records from a file' system into a ring buffer, where said plurality or records comprises a subset of all records in the file system” as data collection begins in the IECs. An IEC is a subroutine that marshals the desired data into a special format and puts it in a shared memory buffer (page 7, paragraph 0111).

data is organized so it's easy to write, since incoming data volume can be very high, and also so it's easy to read directly from disk, since dataset size will typically preclude loading all data into memory (page 8, paragraph 0124). The control station can also specify a reset condition. It can also specify how many events the LEC should store in its circular buffer (e.g. ring buffer) store (page 21, paragraph 0320).

“Scan each record in the ring buffer to identify a user session for said record and to identify any start or end records in the ring buffer” as collection and transmission of dynamic data is expensive, and a filter is scanned for clauses that specifically refer to the dynamic information that is required (page 13, paragraph 0217).

while waiting for a trigger condition to occur, events are retained transiently by the LEC in a circular buffer (e.g. ring buffer) whose size can be specified by VSA. For example, VSA can specify that the buffer store 500 events, so when the 501st event comes in, the first event is written over (page 13, paragraph 0203).

Kaler does not explicitly teach the claimed limitation “allocate, for each identified user session, an index to identify all records in the ring buffer that are associated with the identified user session and to identify all start or end records; and process the index to group all records in the ring buffer belonging to a complete user session, to output the grouped records for further analysis”.

Moran teaches session identifier, this is an index to a data structure specifying the conditions for this particular invocation of this sensor. This data structure includes the host that the sensor collected data from and the options specified for this invocation (page 18, lines 41-45).

the sensor that processes lastlog makes two passes over the file. The file is an array of struct lastlog data structures, indexed by the User ID (column 23, lines 55-57).

the extent can identify the specific user whose records were tampered with depends upon the size of the struct lastlog records and on the pattern of allocation of User IDs on the host (column 24, lines 1-4).

when a valid username-password pair is entered, the login process writes a record to the utmp and wtmp files and updates the lastlog file. The utmp file tracks that are currently logged in and the wtmp file provide a historical record, including both completed login sessions and active sessions (column 19, lines 61-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler to allocate user session and to identify all start or end records because that would allow a system administrator to be alerted whenever an entry matching any of the patterns he has specified is written to a designated log file, thereby substantially reducing his need to manually check the log file as taught by Moran (column 10, lines 43-46).

As to claim 11, Kaler teaches the claimed limitations:

“A system for session-based processing of log files using a data processing system and network session data collected from one or more users” as a method and apparatus for analyzing the performance of a data processing system (page 1, paragraph 0002).

the Visual Studio Analyzer (VSA) includes an efficient mechanism for collecting and transmitting the data to a central log (page 22, paragraph 0339). Logs from multiple machines must be merged and sorted (page 1, paragraph 0015). API for generating events from begins session to end session (page 16 top left, C interface codes).

in the graphical UI, users are presented with three trees, each appearing in a separate window that represents the key information: a Machines/Processes window, a Components window, and a Categories/Events window. The Machines/Processes window presents all of the machines being monitored and the processes on the machines (page 14, paragraph 0230).

Kaler does not explicitly teach the claimed limitation “a log file collection system for collecting a plurality of server request entries, wherein a server request entry comprises a session identifier; a processing engine to process a subset of the plurality of server request entries to group the server request entries by session using the session identifier in each server request entry”.

Moran teaches session identifier, this is an index to a data structure specifying the conditions for this particular invocation of this sensor. This data structure includes the host that the sensor collected data from and the options specified for this invocation (page 18, lines 41-45).

the data collection modules are designed to be lightweight and relatively simple, and different data sources are handled by different modules. These modules extract the data and add identifying information for the fields, simplifying the task for the analysis engine (column 10, lines 12-16).

when a valid username-password pair is entered, the login process writes a record to the utmp and wtmp files and updates the lastlog file. The utmp file tracks that are currently logged in and the wtmp file provide a historical record, including both completed login sessions and active sessions (column 19, lines 61-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler a processing engine to process at least a subset of the plurality of server request entries to group the server request entries by session because that would allow a system administrator to be alerted whenever an entry matching any of the patterns he has specified is written to a designated log file, thereby substantially reducing his need to manually check the log file as taught by Moran (column 10, lines 43-46).

As to claim 14, Kaler does not explicitly teach the claimed limitation “a parser for further analysis the web server request entries that have been grouped by session to generate a user session history”.

Moran teaches a secondary source is provided by the access times on the files related to the user shells: the shell Run Command files indicate the last usage of the shell by that user account, and this typically corresponds to the last login. The access time on the logout RC file and the last-modification time on the shell's history file provide secondary evidence for the last logout on that account (column 23, lines 9-16). Various shells provide a session history mechanism, allowing the user to edit and repeat previous commands. These shells also allow the history to be saved over sessions (column 26, lines 53-56).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler analysis the web server request entries that have been grouped by session to generate a user session history because that would allow the operator to examine the transaction history, but do not provide the context needed to effectively reevaluate the decisions as taught by Moran (column 32, lines 22-24).

As to claim 15, Kaler does not explicitly teach the claimed limitation "the processing engine generates an output file containing web server request entries corresponding to one or more complete user sessions”.

Moran teaches the utmp file tracks who is currently logged in, and the wtmp file provides a historical record, including both completed login sessions and active sessions (column 19, lines 63-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler log file entries corresponding to one or more complete user sessions because that would allow real-time monitoring of larger volumes of traffic as taught by Moran (column 2, lines 56-57).

As to claim 16, Kaler does not explicitly teach the claimed limitation “the processing engine generates an output file containing web server request entries corresponding to one or more incomplete user sessions”.

Moran teaches the file system occasionally gets corrupted, either from a hardware fault or because the system failed to complete a sequence of write operations (column 30, lines 55-57).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler entries corresponding to one or more incomplete user sessions because that would allow real-time monitoring of larger volumes of traffic as taught by Moran (column 2, lines 56-57).

As to claim 17, Kaler does not explicitly teach the claimed limitation “the processing engine generates an output file containing web server request entries corresponding to one or more user sessions that do not include an end session entry”.

Moran teaches the lastlog file contains the time of the last login for each user, and the previous value is written to the user's terminal as part of the hello message. When the user logs out, the getty process removes the corresponding entry from the utmp file and writes a session-end record to the wtmp file (column 19, line 66 to column 20, line 3).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler request entries corresponding to one or more user sessions that do not include an end session entry because that would allow real-time monitoring of larger volumes of traffic as taught by Moran (column 2, lines 56-57).

As to claim 18, Kaler teaches the claimed limitations:

“A system for parsing web site logs one session at a time, comprising: means for storing network session data from at least one server log file” as the VSA includes an efficient mechanism for collecting and transmitting the data to a central log (page 22, paragraph 0339).

data objects, which can be used to access different types of data, including web pages, spreadsheets, and other types of documents (page 4, paragraph 0072).

“Means for reading a subset of the network session data” as BeginSession is called by an entity before it fires events to register its entity and instance names (source and session). EndSession is called by an entity after it completes firing events (page 1, paragraph 0251-0252).

“Means for processing the subset of the network session data to group said network session data by session” as the set of APIs includes an interface that enables the operating system to read any one or more of several fields in the application. These fields include arguments, source machine, source process, source session and target session (page 15, paragraph 0246).

“Means for generating a first output file containing network session data grouped by session” as API for generating events from begin session to end session (page 16 top left, C interface codes).

“Means for parsing said first output file” as implementations involve writing data to disk. Even if the input/output (I/O) is buffered asynchronously (page 1, paragraph 0012). All of the log files would need to be collected, merged, and sorted. The developer would then have to sift through the data in a time-intensive fashion (page 1, paragraph 0009).

Although kaler teaches data objects which can be used to access different types of data, including web pages (page 4, paragraph 0072).

Kaler does not explicitly teach the claimed limitation “a system for parsing web site”.

Moran teaches computer network also includes an Internet access server configured to enable users of host computer systems connected to the computer network to access the Internet and in particular to access web pages via the World Wide Web by sending and receiving hypertext transfer protocol (HTTP) transmissions (column 7, lines 20-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler and Moran before him/her, to modify Kaler a system for parsing web site because that would allow real-time monitoring of larger volumes of traffic as taught by Moran (column 2, lines 56-57).

6. Claims 9 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaler et al. (US Patent Application No. 2003/0061541 A1) as applied to claims 8 and 11 above, and further in view of Moran (US Patent No. 6,826,697 B1) and Balsamo et al (US Patent Application No. 2002/0099806 A1, hereinafter "Balsamo").

As to claim 9, Kaler does not explicitly teach the claimed limitation "the index comprises: a session record for each identified user session for keying into the ring buffer to identify log records associated with said identified user session; a hash table for keying into the session record based upon session key information; a linked listing of last seen log records for each session; and a linked list of first seen log records for each session".

Moran teaches session identifier, this is an index to a data structure specifying the conditions for this particular invocation of this sensor (page 18, lines 41-44).

Also, Balsamo teaches a data collection system includes a processor and a memory storing a computer program product for execution in the processor. The computer program product removes duplicate records produced from gathering statistics concerning network data packets and includes instructions to determine whether a session key associated with the network record maps to an active session (page 1, paragraph 0008).

if the network accounting records (NAR) type could have several records in a session, then the order node will need to process the NAR and keep track of the NAR. The order node process will make a time stamp. The session table, which can be implemented as a hash table, will store the session key and a time (page 9, paragraph 0097).

the chaining of the nodes provides a data flow architecture in which input data/records are fed to the first node in the chain and the output records/data from the nodes are received from the last node of the chain. The data that is processed by each node is processed in an order in which nodes are arranged in the chain (page 2, paragraph 0034).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler, Moran and Balsamo before him/her, to modify Kaler a hash table for keying into the session record based upon session key information because that would allows user to specify which nodes are to receive output NARS from the node as taught by Balsamo (page 7, paragraph 0079).

As to claim 12, Kaler teaches the claimed limitations:

“A ring buffer for storing the subset of the plurality of web server request entries” as the control station can also specify filters, for example a first filter and a second filter. The control station can also specify a reset condition. It can also specify how many events the LEC should store in its circular buffer (e.g. ring buffer) store (page 21, paragraph 0320).

Kaler does not explicitly teach the claimed limitation “the processing engine uses a plurality of data structures to group the web server request entries by session, said plurality of data structures comprising: a per-session record for keying into the ring buffer, a hash table for keying into the per-session records, a linked list of last processed web server request entries for each session, and a linked list of first processed web server request entries for each session".

Moran teaches computer network also includes an Internet access server configured to enable users of host computer systems connected to the computer network to access the Internet and in particular to access web pages via the World Wide Web by sending and receiving hypertext transfer protocol (HTTP) transmissions (column 7, lines 20-25).

session identifier, this is an index to a data structure specifying the conditions for this particular invocation of this sensor (page 18, lines 41-44).

Also, Balsamo teaches a data collection system includes a processor and a memory storing a computer program product for execution in the processor. The computer program product removes duplicate records produced from gathering statistics concerning network data packets and includes instructions to determine whether a session key associated with the network record maps to an active session (page 1, paragraph 0008).

if the network accounting records (NAR) type could have several records in a session, then the order node will need to process the NAR and keep track of the NAR. The order node process will make a time stamp. The session table, which can be implemented as a hash table, will store the session key and a time (page 9, paragraph 0097). The chaining of the nodes provides a data flow architecture in which input data/records are fed to the first node in the chain and the output records/data from the nodes are received from the last node of the chain. The data that is processed by each node is processed in an order in which nodes are arranged in the chain (page 2, paragraph 0034).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler, Moran and Balsamo before him/her, to modify Kaler a hash table for keying into the session record based upon session key information because that would allows user to specify which nodes are to receive output NARS from the node as taught by Balsamo (page 7, paragraph 0079).

7. Claims 10, 13, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaler et al. (US Patent Application No. 2003/0061541 A1) as applied to claims 8, 11 and 18 above, and further in view of Moran (US Patent No. 6,826,697 B1) and Clark (US Patent No. 6,965,634 B1, hereinafter “Clark”).

As to claim 10, although Kaler teaches while waiting for a trigger condition to occur, events are retained transiently by the LEC in a circular buffer whose size can be specified by VSA. For example, VSA can specify that the buffer store 500 events, so when the 501st event comes in, the first event is written over (page 13, paragraph 0203).

Kaler does not explicitly teach the claimed limitation “the ring buffer implements a sliding window to process all of the log records in the file system into complete user sessions by sequentially adding and removing log records to the ring buffer until all of the log records in the file system have been processed”.

Clark teaches this span of time is called the time uncertainty window; and the operation of redefining the past and future edges of the window, and updating the stored timing data accordingly, is called sliding the window (column 9, lines 15-19).

a method of updating a linked list uses time indexes that are modulo incremented and an old index value instead of using pointers, where array information is stored in a circular buffer and the old index value is updated to manage an end of the list (column 3, lines 20-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler, Moran and Clark before him/her, to modify Kaler the ring buffer implements a sliding window because that would allowing an authorized receiver acquire some timing information as taught by Clark (column 3, lines 14-16).

As to claim 13, Kaler does not explicitly teach the claimed limitation "the processing engine uses a sliding memory window to process the subset of the plurality of web server request entries".

Clark teaches this span of time is called the time uncertainty window; and the operation of redefining the past and future edges of the window, and updating the stored timing data accordingly, is called sliding the window (column 9, lines 15-19).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler, Moran and Clark before him/her, to modify Kaler the ring buffer implements a sliding window because that would allowing an authorized receiver acquire some timing information as taught by Clark (column 3, lines 14-16).

As to claim 19, Kaler does not explicitly teach the claimed limitation "means for reading a subset of the network session data comprises a sliding window".

Clark teaches this span of time is called the time uncertainty window; and the operation of redefining the past and future edges of the window, and updating the stored timing data accordingly, is called sliding the window (column 9, lines 15-19).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, having the teachings of Kaler, Moran and Clark before him/her, to modify Kaler the network session data comprises a sliding window because that would allowing an authorized receiver acquire some timing information as taught by Clark (column 3, lines 14-16).

As to claim 20, Kaler teaches the claimed limitations:

"Means for reading a subset of the network session data comprises a ring buffer" as while waiting for a trigger condition to occur, events are retained transiently by the LEC in a circular buffer (e.g. ring buffer) whose size can be specified by VSA (page 12, paragraph 0203).

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Hwa whose telephone number is 571-270-1285. The examiner can normally be reached on 8:00 – 5:00. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Don Wong can be reached on 571-272-1834. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.
Status information for unpublished applications is available through Private PAIR only, for more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the PAIR system contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

06/16/2008

/James Hwa/

Examiner, Art Unit 2163

/Cam Y Truong/
Primary Examiner, Art Unit 2162